Google Cloud's
Approach to Security

Google Cloud

Table of **Contents**

Google Cloud

2

Staying One Step Ahead.

Protecting a global network against persistent and constantly evolving cyber threats is one of the most important challenges we face. At Google, it's all in a day's work: data centers in the United States, South America, Europe, and Asia support billions of users in the public and private sectors.

Google's global network protects seven different global businesses, each with over 1 billion customers, including popular Google services such as Google Search, YouTube, Maps, and Gmail. We also work to protect the data and operations of thousands of advertising and media companies that rely on Google's ad products to run their business. Safeguarding our services, our infrastructure, and our users' data is core to our continued success. To stay ahead, we've not only adopted industry best practices, we've also led the technology industry in security by developing advanced tools and strategies of our own.

Our network communications protocols—the rules that enable communications between systems—change multiple times per second to

make malicious intrusions much harder. Data in Google Cloud is encrypted both in transit and at rest. Google's network capacity far exceeds any traffic load we host, so if a distributed denial-of-service (DDoS) attack—where attackers try to shut down a service by flooding the network with traffic—occurs, we can continue serving traffic while we work to isolate and shut down the source of the attack. Numerous other products, tools, and processes work to provide defense in depth.

Our commitment to security underpins everything we do. It extends from our platform and infrastructure to our software solutions and purpose-built hardware, and gives Google customers the assurance that their data and applications meet security and compliance standards.

This e-book provides a detailed overview of our approach to security and privacy—so you have the data you need to trust us with your most important data and applications.

 Google Cloud

Google Security by the Minute

10 million

spam messages are prevented from reaching Gmail customers

694,000

indexed Web pages are scanned for harmful software

7,000

deceitful URLs, files, and code in browser extensions are stopped

6,000

instances of unwanted software are reported to Chrome users

1,000

instances of suspected malware are reported to Chrome users

2

phishing sites and 1 malware site are identified and mitigated

Research Spotlight:
The Future of Security in the Public Cloud

In new research from McKinsey & Company, to which the Google Cloud security team contributed expertise, a majority of the 100 enterprise organizations surveyed expect to double their public cloud adoption in the next three years—going from 19% of workloads to 38%. One organization predicted a future in which more than 90% of workloads have been migrated to the cloud.

Another learning from the research: In a hybrid, multi-cloud world, organizations can't simply extend on-premises security controls to the public cloud, where configurations and workflows are different. They need to work closely with cloud providers to implement a shared, end-to-end security model.

Google Cloud

Raising the Bar

01

Google Cloud

A Security-
Obsessed Culture

More than 850 security professionals within Google monitor, design, research, and engage with the wider global community of Internet professionals and users. They uncover vulnerabilities, report software bugs to software vendors, and design new security solutions and approaches.

Security is incorporated into the entire software development process at Google. This includes analysis of architectures and code to uncover vulnerabilities and potential attack models for a new product or feature. Our dedicated Incident Management Team ensures that any incidents that do arise are quickly addressed, analyzed, and remediated with minimal disruption to our customers.
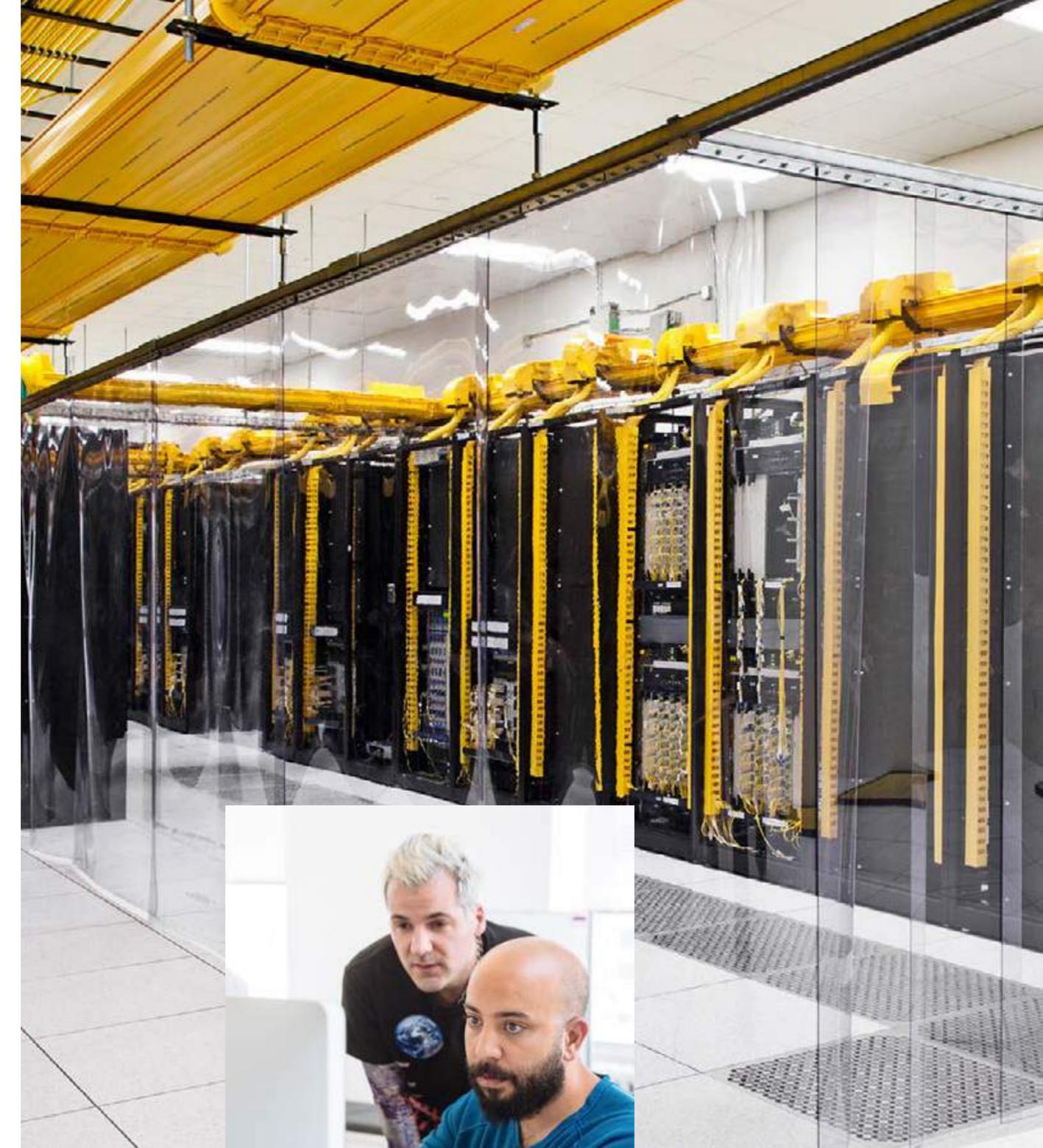
Google Cloud

Threat Prevention and Detection

Effectively preventing cyber threats from impacting Google Cloud requires vigilance, innovation, and agility—and sophisticated detection capabilities. Years of handling much of the Internet's traffic, combined with investments in artificial intelligence, large data sets, and global-scale infrastructure, have all contributed to our success in continually safeguarding our network.

Corporate webmasters and application developers get direct notification of malicious attacks, as well as diagnostic tools to monitor their network. Google's research into phishing attacks resulted in the development of security keys, small, easy-to-use hardware devices that employ public-key cryptography for strong authentication. They help protect user accounts across Google Cloud services, including both Google Cloud Platform and G Suite.

Corporate customers benefit from our years of experience working to secure devices like Google Chromebooks. They were designed with many of the same security principles that went into Google data centers. Features and practices like deep identity management, minimal data exposure, and centralized device control add up to a high level of threat prevention.

A Global Security Pioneer

Google has published close to 300 papers on security, privacy, and abuse prevention. We have also distributed many tools for improving software security industry-wide. Many of these tools, along with many more software applications, are released as open source in order to support the community and encourage the highest possible rate of innovation. We have donated more than 20 different software projects to open source, promoting better security practices, and have fixed more than 100 security bugs in open-source Linux and Chrome.

Perfect Forward Secrecy

Google is the first major cloud provider to enable perfect forward secrecy. This feature provides a greater measure of protection for encrypted communications. It makes it more difficult for attackers to compromise secret keys or passwords. The service has been available since 2011 to users of Gmail, Google Docs, and encrypted Search.

Google Cloud

Rethinking Secure Remote Access

A massive project at Google reimagined how we provide employees with secure remote access to applications. It resulted in BeyondCorp, Google's innovative zero-trust security model. Instead of assuming a person or a machine is inside or outside of the network, the model uses computation to allow access to individual services as needed, based on trusted identities and devices. Every day, thousands of our employees can work securely with Google's core infrastructure from any location. They do not use a traditional and less-secure VPN.

Our zero-trust model is what allows Google employees to sign into any laptop, from anywhere, with secure authentication tied to the user instead of the network. It means work can happen anywhere, seamlessly and securely—powering higher levels of trust and productivity. Administrators retain control of policies that determine which resources are authorized for use by whom.

Stronger Encryption

To protect against threats to encryption techniques based on cryptographic advances, in 2013 Google decided to double our RSA encryption key length to 2048 bits. We also change our key every few weeks.

In 2017, Google Trust Services was established to operate our own Root Certificate Authority to issue digital certificates. A digital certificate acts as a trusted third party to certify the ownership of a public key, part of the widely used X.509 cryptography standard used in communications.

Google Cloud

Secure by Design

Google Cloud

02

Secure by Design

At Google Cloud, we manage security throughout the data life cycle, from the data center to the device. Our customers extend their own enterprise security measures into the cloud in a collaborative model. Google Cloud security uses a range of technologies, approaches, standards, and methodologies to protect applications, IT resources, and customer data.
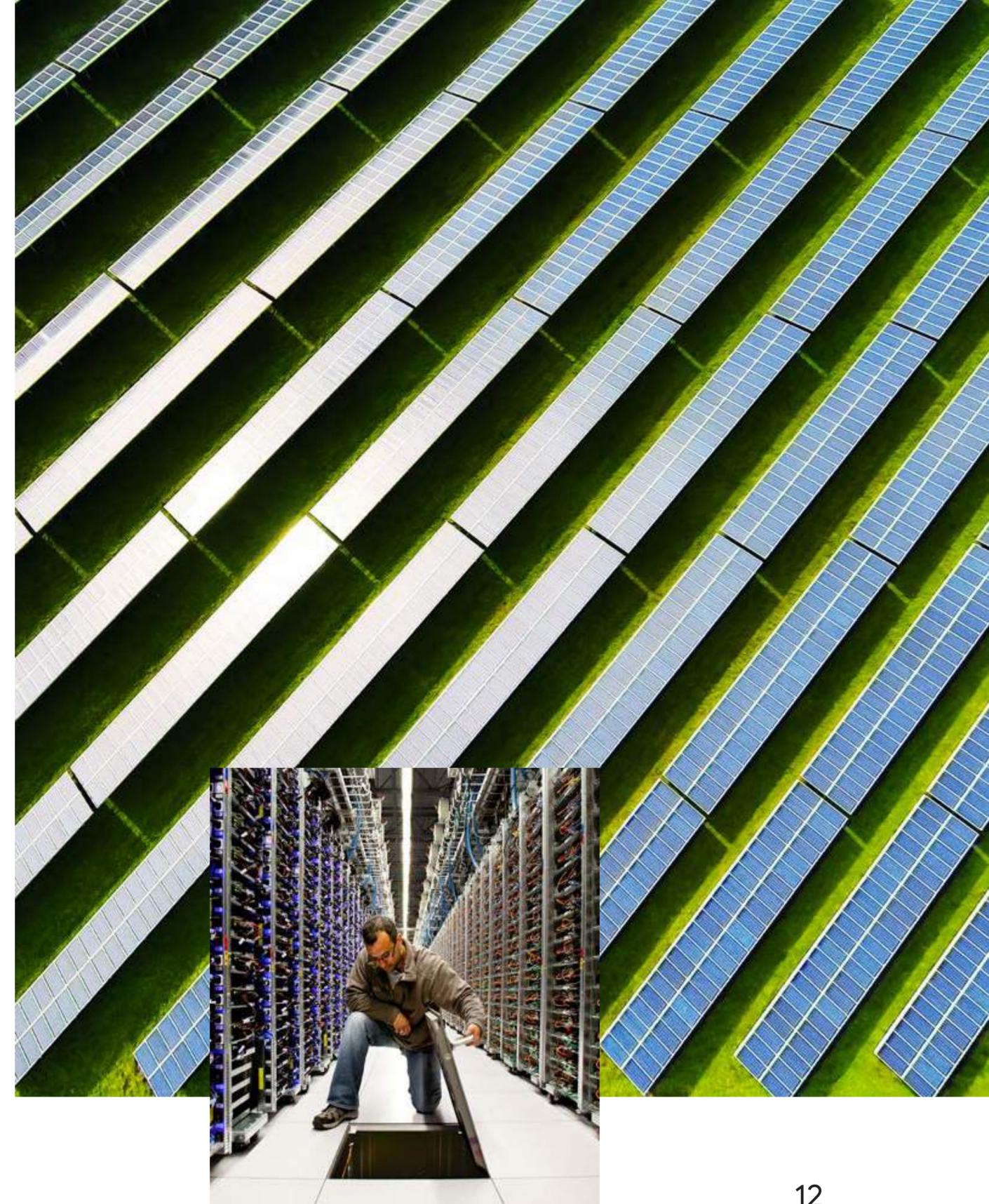
Google Cloud

Multilayered Approach

Google Cloud Platform's infrastructure security is designed in progressive layers—hardware, services, user identity, storage, internet communication, and operations. We call this *defense in depth*. Each layer has strict controls for access and privileges. From physical data center components to hardware provenance, secure boot, secure inter-service communication, secured data, and protected access to services from the internet, Google Cloud's approach to security is highly effective and continually evolving. Security layers are augmented by the technologies and people processes Google deploys for operational security.

Facility and Hardware Security

Access to Google data centers is limited to a small number of specially qualified Google employees. We use multiple physical security layers to protect each floor. They include technologies like biometric identification, metal detectors, cameras, physical barriers, and laser-based intrusion detection.

Our data centers have thousands of server machines connected to a local network, providing an initial security layer. Both the server boards and networking equipment are custom-designed by Google to adhere to our tough security requirements. We audit and validate the security properties of component vendor products we use. Google's custom-designed chips include Titan, a hardware security chip deployed on both servers and peripherals that allows us to identify and authenticate legitimate Google devices at the hardware level.

Google Cloud

Secure Boot Stack and Machine ID

Google server machines use a variety of technologies to ensure that they are booting the correct software stack. They are all built, controlled, and hardened by Google engineers and are continually evolving to enhance security. Automated systems ensure that servers run up-to-date software versions, including security patches, to diagnose hardware and software problems and remove machines from service if necessary.

Each server machine has its own specific identity that can be tied to the hardware root of trust and the software booted by the machine. So every time a machine communicates with the Google Cloud network, its individual identity is verified.
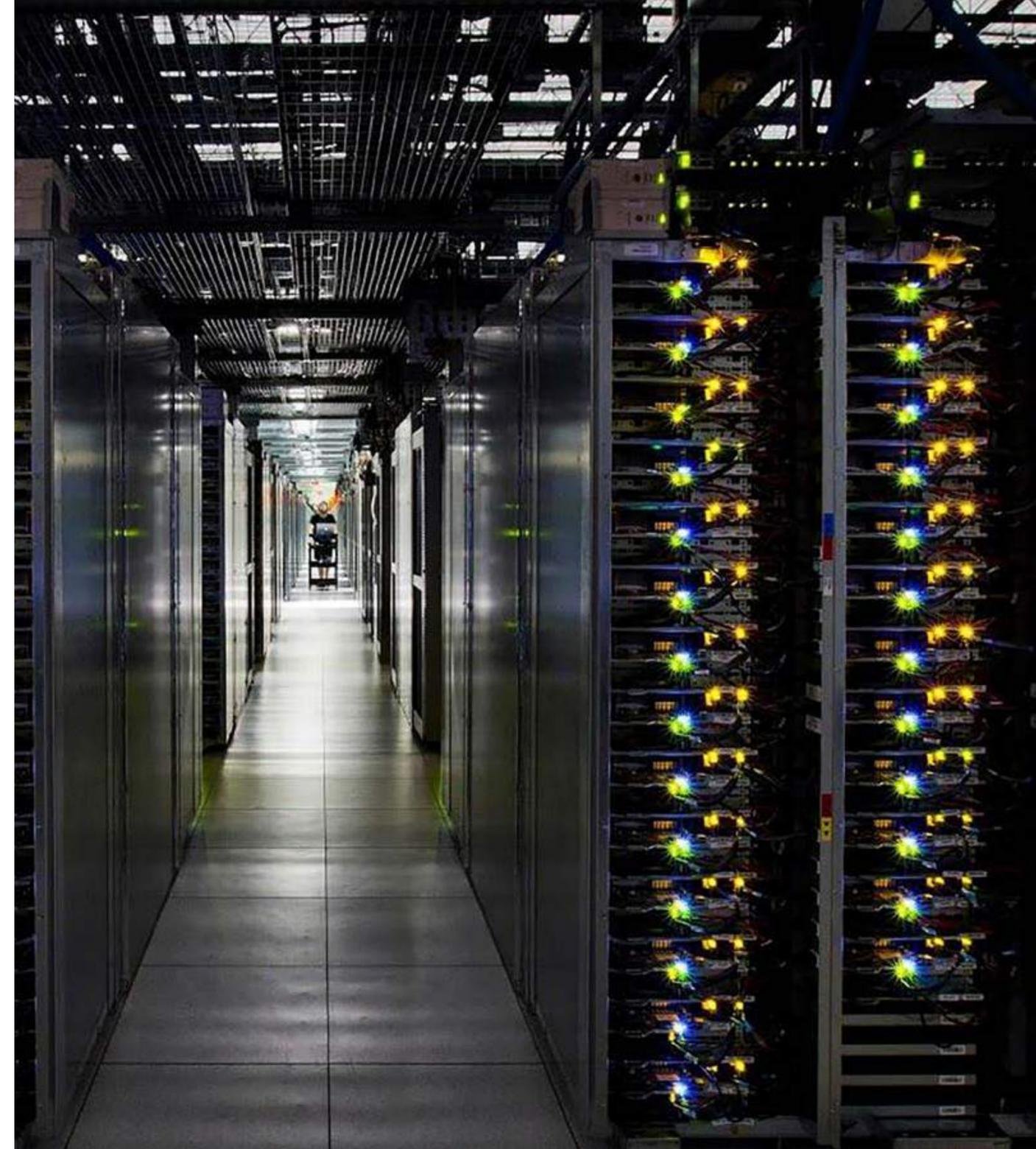
Google Cloud

Service Identity, Integrity, and Isolation

Google Cloud uses sophisticated techniques like cryptographic authentication and authorization at the application layer for services such as computing, data storage, data analytics, and machine learning. This means that services may be run on thousands of machines to handle the required scale of the workload, and that they are controlled by a cluster orchestration service to be optimally efficient and available when you need them.

Internal network segmentation—restricting infrastructure use to only those network assets required to perform a particular job—and the use of specialized security appliances like firewalls are not the primary security mechanisms used on Google Cloud Platform, although ingress and egress filtering are used to prevent IP spoofing. Traditional perimeter security, with its intrinsic trust of everyone inside, is less effective in companies where employees work both onsite and offsite. To allow work to happen anywhere, anytime, we take a different approach.

Each service has an associated service account identity and is provided with cryptographic credentials, used by servers and clients, that are used to prove its identity. Google source code—the fundamental software programs behind our many solutions—is stored in a central repository where all versions are auditable.

Google Cloud

Inter-Service Access Management

Google Cloud customers using specific services from the platform can customize and manage them. Using a console, they can specify and restrict what other services can communicate with their services. For example, using application programming interfaces (APIs), an analytics back-end applications can be added to an enterprise resource planning (ERP) app. Or the APIs can be used to allow access to the service only for certain users based on their account identities.

Google engineers are also issued individual identities, so services can be configured to allow or deny them access. The infrastructure also provides services the ability to read from central access control list (ACL) and group databases, which verify user and access privileges through still other security measures.

Our software runs in Google's containers, a resource-efficient technique for deploying applications from within an operating system without the need to launch virtual machines. Aside from resource efficiency, containers enable system-wide management and lightning-fast system audits. Configuration changes and security patches can be deployed everywhere, quickly, with minimal downtime. We offer our customers an open-source version of these containers called Kubernetes. Using containers, you can quickly access secure and sensitive data logs required in compliance audits. This used to take days; now it's done in minutes.

Google Cloud

Encryption of Inter-Service Communication

Our infrastructure also provides cryptographic privacy and integrity for remote procedure call (RPC) data over the WAN between data centers. RPCs are communications between programs on different networks that request services. To protect against sophisticated adversaries who may be trying to tap our private WAN links, the infrastructure automatically encrypts all infrastructure RPC traffic.

Cryptography is the science of using math to encrypt and decrypt data. At Google, we use it to ensure that RPC data moving on the network is private, unchanged by any third party, and is being exchanged between trusted partners. These cryptographic features are encapsulated inside of the the Google Cloud RPC mechanisms so they are available to other application-layer protocols such as HTTP. This provides application-layer isolation and removes dependency on the security of the network path. Encrypted inter-service communication can remain secure even if the network is tapped or a network device is compromised.
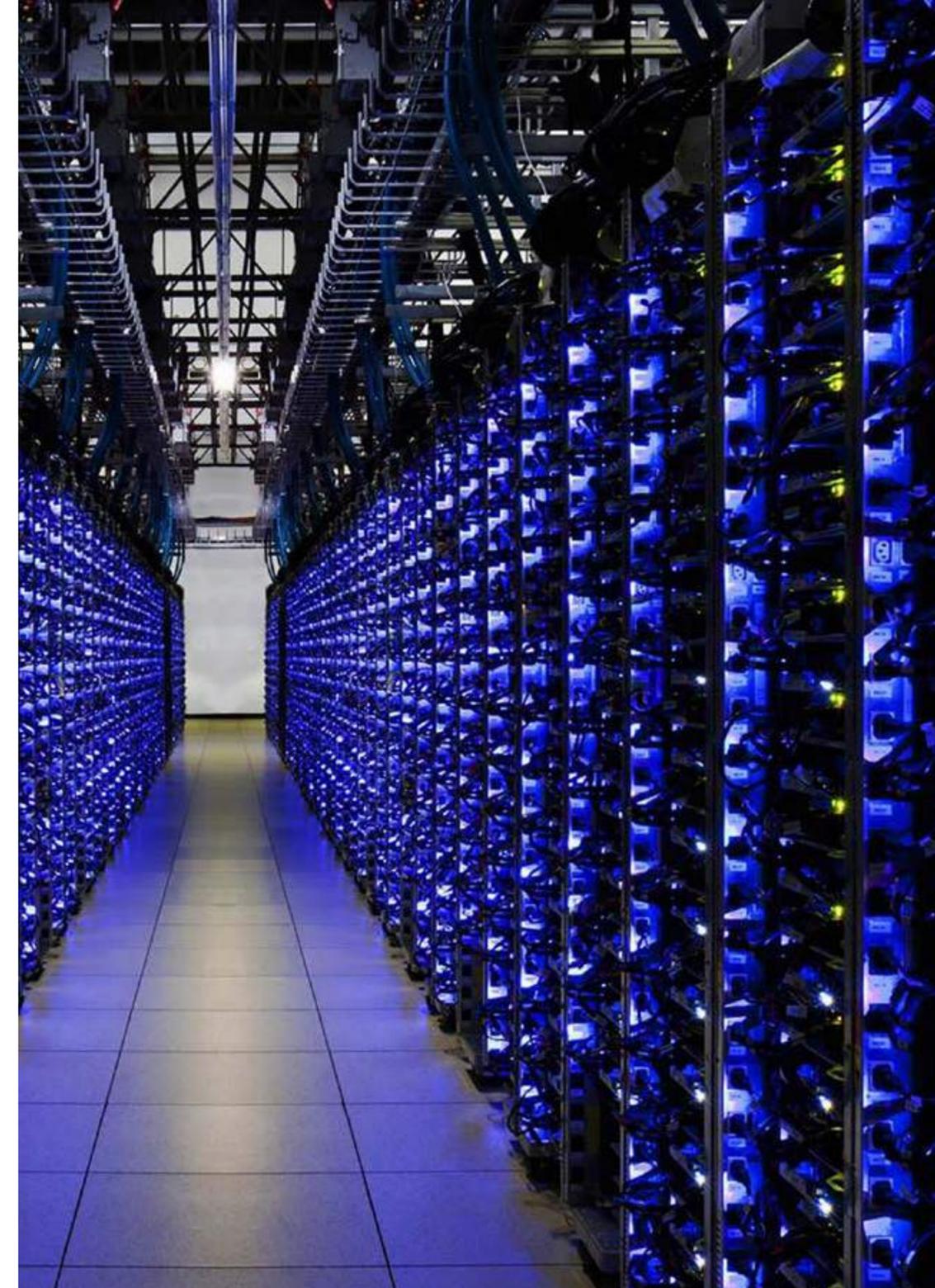
Google Cloud

Access Management and Transparency of End User Data

Google Cloud's infrastructure provides a central user identity service that issues end user permission tickets as part of the RPC. The tickets prove that a service is responding to a request on behalf of a particular end user.

An end user login is verified by the central identity service, which then issues a user credential (such as a cookie or OAuth token) to the user's client devices. Every subsequent request from the client devices into Google Cloud needs to present that user credential.

In 2017, Google partnered with SAP to implement a joint data custodian model. The model offers SAP as custodian of customer data on Google Cloud, with continuous monitoring for compliance, based on defined controls.

Secure Data Storage

The various Google storage services can be configured to use keys from a central key management service to encrypt data before it is written to physical storage. Performing encryption at the application layer allows the infrastructure to isolate itself from potential threats at the lower levels of storage such as malicious disk firmware. Other layers of protection are also used, such as hardware encryption.

Secure Internet Communication

Google Cloud secures communication between the internet and Google Cloud services. We isolate our infrastructure into a private IP space, exposing only a subset of machines directly to external internet traffic and DDoS attacks. Other features, like Google Cloud Armor—available with the use of Cloud Load Balancer—are used to provide DDoS protection at the network edge, closer to the origination of attacks.

The Google Front End (GFE) services ensure that all transport layer security (TLS) connections are terminated using correct certificates and follow best practices. The GFE also provides protections against DDoS attacks. Here's how it works: Load balancers report information about incoming traffic to a central DDoS service. If it detects that a DDoS attack is occurring, it can configure the load balances to drop or throttle the traffic. The GFE layer also reports information about DDoS, including application layer information, and the GFE can also be configured to drop or throttle traffic if a DDoS attack is detected.

Our central identity service, which users see as the Google login page, asks for a username and password, and assesses risk factors such as whether users have logged in from the same device or location in the past. The service issues credentials such as cookies and OAuth tokens. Second factors, such as one-time passwords or phishing-resistant security keys, may also be used by users when signing in.

Google Cloud

Operational Security

Our security teams triage, investigate, and respond to incidents 24 hours a day, 365 days a year. We conduct regular exercises to measure and improve security detection and response. Google Cloud provides libraries and frameworks that prevent developers from introducing certain classes of security bugs, like XSS vulnerabilities in web apps. Automated tools are available to detect security bugs, including fuzzers, static analysis tools, and web security scanners. Manual security reviews are also used. Conducting these efforts manually on an ongoing basis would be cost-prohibitive and time-consuming to a typical enterprise organization.

Google makes a heavy investment in protecting our employees' devices and credentials from compromise using technologies and strict policies for physical, computer, data, and network security; access management; security logging; and more. We also monitor activity to discover potential compromises and illicit insider activity. Application-level access management controls expose internal applications only to specific users. Administrative access privileges are limited and monitored. And sophisticated intrusion detection utilizes host-based signals on individual devices, network-based signals from various monitoring points, and signals from infrastructure services.

Google Cloud

Compliance and Trust

03

Google Cloud

Meeting Global Security Standards

As a global network, Google adopts the network, data, privacy, and operational policies set by nations where we operate so Google Cloud customers can meet policy, regulatory, and business requirements and compliance mandates. We follow industry standards, including those of the International Organization for Standardization (ISO), the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC) 2 and 3; the Payment Card Industry Data Security Standard (PCI DSS); the National Institute of Standards and Technology (NIST); and many others.

Google Cloud

Meeting Rigorous Privacy and Compliance Standards

Google Cloud is committed to complying with the European Union's General Data Protection Regulation (GDPR). GDPR strengthens the rights of individuals over their personal data and seeks to unify data protection laws across Europe. Additionally, Google Cloud has produced documentation as to how we adhere to the Australian Privacy Principles (APPs) and Australian Prudential Regulation Authority (APRA) Standards, the Japan Center for Financial Industry Information Systems (FISC) guidelines, the Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584, the Spain Esquema Nacional de Seguridad (ENS) accreditation scheme, and the UK NCSC Cloud Security Principles.

Trust-First Approach

The Google Cloud Trust Principles summarize our commitments to protecting the privacy of customer data. The customer—not Google—owns their data. You decide how it resides in Google Cloud, applying factors such as data segregation, controls by region, key encryption, and revocation. And if you choose to stop using Google Cloud, you can take your data with you at any time.

Google Cloud

Going Beyond Enterprise Protections

The scale of Google Cloud operations and our collaboration with the security research community let us either address vulnerabilities quickly or prevent them proactively. By extending their own enterprise security measures into Google Cloud in a collaborative partnership model, our customers not only gain protection, they can generate new revenue by offering new services and business models.

London-based financial technology company Ravelin has become a major player in online fraud prevention through the use of the artificial intelligence technique called machine learning. Google Cloud's commitment to open source technology allowed Ravelin to migrate its entire infrastructure onto the Google Cloud Platform. Google Cloud's

strong security and cutting-edge encryption allow Ravelin to more safely store and analyze credit card details, location data, and personal identifiable information for its clients, in compliance with ISO/IEC 27001 and Payment Card Industry Data Security Standards (PCI DSS). Ravelin's anti-fraud machine learning model processes transactions within 300 milliseconds. As of 2017, the company has stopped over £100 million of fraudulent transactions and analyzed over 12 petabytes of data over a three-year period.

A Globally Distributed Network

Google provides services that can be accessed by millions of users no matter where they are. Google Cloud services operate globally, using a geographically distributed infrastructure to help ensure that the services that run on them have maximum availability and uptime. Data typically no longer resides on a single hard drive or server rack, or even in a single data center. Instead, it must be stored, secured, and made available so it can be accessed by the users who depend on it in India or Oklahoma just as easily as in New York or Germany. This dependable, 24/7 availability, along with Google Cloud security, best practices for secure data handling, and adherence to compliance mandates, are behind the growing popularity of Google Cloud among enterprise organizations worldwide.
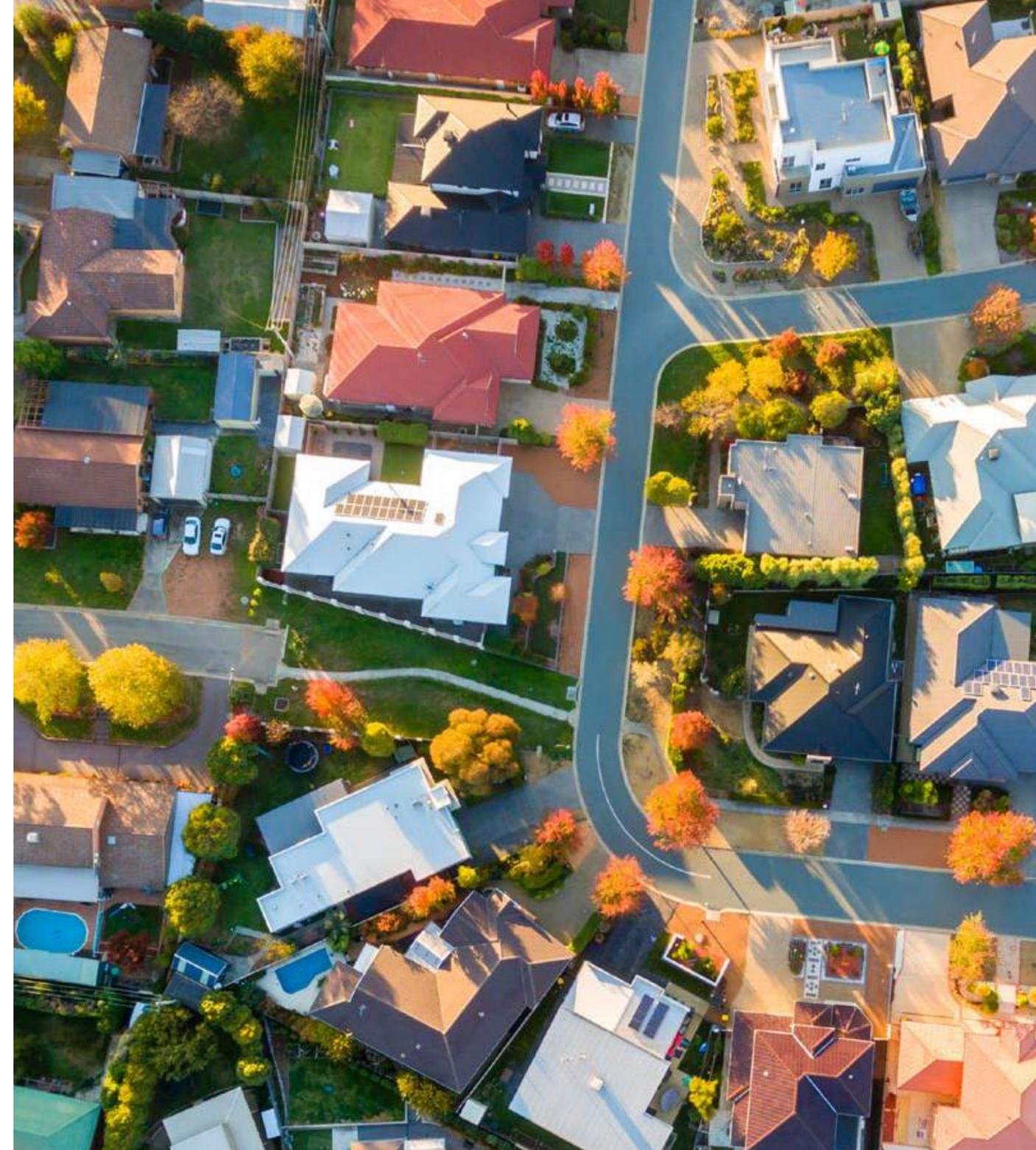
Google Cloud

Conclusion

Three Tenets
of Google Cloud

We protect your business through a collaborative process designed to help you make the right people, process, and technology adjustments to keep up with new threats and security challenges. By choosing to work with the cloud built on the world's largest computing network infrastructure, your organization will gain access to our expertise, our experience, and the agility to address the threats of today and tomorrow. As a Google Cloud customer, you'll get to use the same infrastructure that has propelled and sustained Google, including the power of machine learning, AI, and IoT.

You maintain control over your data, with the power to determine how it is collected and used by providers, employees, and your customers. Google Cloud is committed to providing customers with data transparency and controls to manage access. Google's international security and privacy standards are certified and validated by independent auditors. And Google Cloud does not and will not sell any customer data, ever.

We work hard to meet global security standards that support compliance with internal policies and external regulations that may be required by your organization. This includes how data is collected, used, and accessed. The rich set of controls and capabilities supported by Google Cloud continues to grow over time. This includes SSAE 16/ISAE 3402 Type II, ISO 27001/27017/27018, FedRAMP, PCI DSS, HIPAA, CSA STAR, MTCS Tier 3, GDPR (Europe), NIST 800-171/800-53, FISC (Japan), MPAA, SOX, Australian Privacy Act and APPs, APRA Standards, and ENC (Spain).

Google Cloud

For more information, [visit our website](#) to learn more about our security approach.

Google Cloud